بسم الله الرحمن الرحيم

الحمدلله معز الاسلام بنصره ومذل الشرك بقهره ومصرف الامور بأمره ومستدرج الكافرين بمكره الذي قدر الايام دولا بعدله وجعل العافية للمتقين بفضله والصلاة والسلام علي من أعلي الله منار الاسلام بسيفه وعلي اله وصحبه ومن تبعهم باحسان الى يوم الدين اما بعد



[مدخل إلى نظام Qubes OS]

❐ ماهو نظام Qubes OS ؟

هو نظام حر مجاني ومفتوح المصدر مبني علي لينكس ويسمح للمستخدمين بالتحكم الكامل في نظام التشغيل حيث يعد من أفضل أنظمة التشغيل من ناحية الأمان

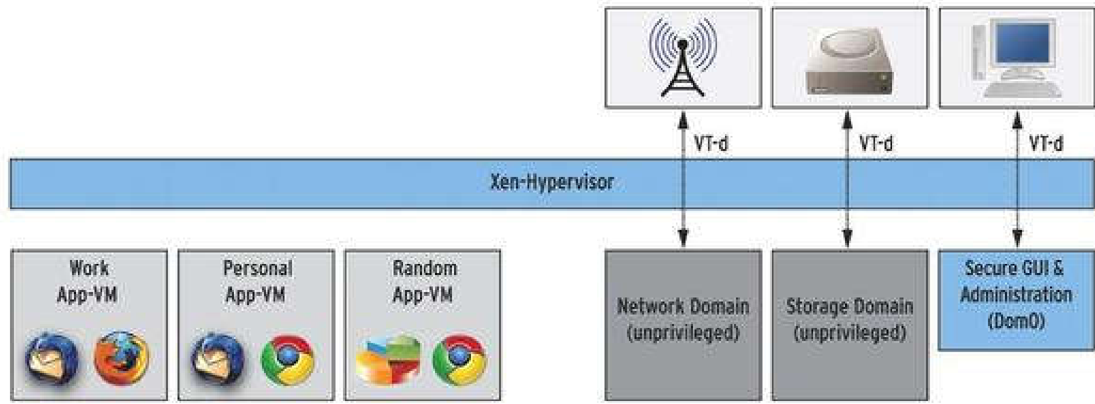
العديد من المناصرين يستخدمون أنظمة تشغيل **مايكروسوفت ويندوز** أو **OS X** علي حواسيبهم الشخصية , وهذه الانظمة مشهورة لانها سهلة الاستخدام وغالبا ما تأتي مثبتة بشكل افتراضي في معظم الحواسيب لكن عند الحديث حول الأمان فعلي سبيل المثال اذا فتحت ملحقات البريد الالكتروني من نظام ويندوز او موقع الكتروني بدون إدراك فانك تسمح بتثبيت برمجيات خبيثة تعمل علي حاسوبك ويمكن لهذه البرمجيات أن تفعل اي شيئ بنظام التشغيل بدءا من اظهار الاعلانات وحتي مزامنة كل حرف تكتبه علي لوحة المفاتيح وبالتالي اختراق النظام

❐ أليس مكافحات الفايروسات و الجدران النارية كافية لحماية المستخدمين ؟

للأسف مكافحات الفايروسات والجدران النارية لم تعد كافية للحماية من الهجمات المعقدة علي سبيل المثال في هذه الايام من الشائع جدا ان يقوم الهاكرز بفحص البرمجية الخبيثة التي قاموا بتطويرها من قبل مكافحات الفايروسات قبل إرسالها الي الضحايا او الاهداف وأفضل مكافح فايروسات غالبا يرصد هذه البرمجيات بعد تحديث قاعدة البيانات والتي قد تستغرق بعض الايام حتي رصده للفايروسات الجديدة مما يجعل نظام التشغيل مخترق طيلة هذه الايام

❐ كيف يوفر نظام Qubes OS حماية أفضل ؟

نظام **Qubes** يعمل علي تقسيم نظام التشغيل من خلال عزل كل جزء عن الاخر وذالك يجعل الاشياء المختلفة التي تفعلها علي جهاز الحاسوب منعزلة بشكل آمن عن بعضها البعض من خلال نوافذ وهمية تسمي " **Qubes** " وذالك حتي اذا اخترقت نافذة وهمية معينة لا يمكنها التأثير علي نظام التشغيل بشكل عام علي سبيل المثال يمكنك انشاء نافذة وهمية لتصفح بعض المواقع الغير آمنة ويمكنك انشاء نافذة اخري للشراء بشكل آمن من خلال شبكة الانترنت وبهذه الطريقة لو أن النافذة الوهمية الخاصة بالتصفح غير الآمن اخترقت لا يمكن للمهاجم الوصول للنافذة الوهمية الاخري الخاصة بالشراء



- جميع النوافذ الوهمية المعزولة مضمنة داخل نظام تشغيل واحد حيث أن جميع البرامج التي تعمل داخل النوافذ الوهمية في نظام Qubes معزولة بشكل تام داخل النافذة الوهمية لكن جميع النوافذ تظهر ضمن واجهة رسومية واحدة ومحددة بالوان مختلفة ليسهل علي المستخدم التمييز بين النوافذ الوهمية ودرجة أمانها

- نظام **Qubes OS** يعزل الاجهزة المتصلة عن طريق ال**USB** وكروت الشبكة من خلال نافذة وهمية (**Qube**) وذالك للحفاظ علي نظام التشغيل من الاختراق

- كما يدعم نظام **Qubes** تشفير جميع الإتصالات عبر شبكة الإنترنت من خلال تمرير الاتصال بشبكة **تور Tor** والتي تخفي هوية المستخدمين وتجعل عملية تعقبهم اصعب

- يدعم نظام **Qubes** تثبيت نواة توزيعات لينكس الأخري مثل **Archlinux , Debian , Fedora**لتثبيتها داخل قوالب الالات الافتراضية ليتمكن المستخدم من تشغيل البرمجيات الخاصة بتوزيعات لينكس داخل نوافذ وهمية كما يدعم تثبيت أنظمة ويندوز داخل قوالب الالات الافتراضية لاستخدام برمجيات ويندوز داخل النوافذ الوهمية

.. ..

AppVMs (Qubes) and TemplateVMs➤

| تطبيقات النوافذ الوهمية وقوالب الآلات الافتراضية |

بنظام **Qubes** يمكنك تشغيل جميع البرامج داخل نافذة وهمية او إفتراضية تسمي **Qubes** لكن ليس كل تطبيق يستخدم نافذة وهمية (فذالك سيستهلك العديد من مصادر الجهاز) لكن كل نافذة وهمية أو **Qube** تمثل نطاق أمني (**Security Domain**) مثل نطاق أمني للعمل أو للاستخدام الشخصي أو للشراء عبر الإنترنت) , لكن جميع النوافذ الوهمية (**Qubes**) مبنية علي قالب الالة

الإفتراضي **Template VM** وعلي الرغم من ذالك يمكن للمستخدم انشاء المزيد من قوالب الالة الافتراضية (**TemplateVM**)

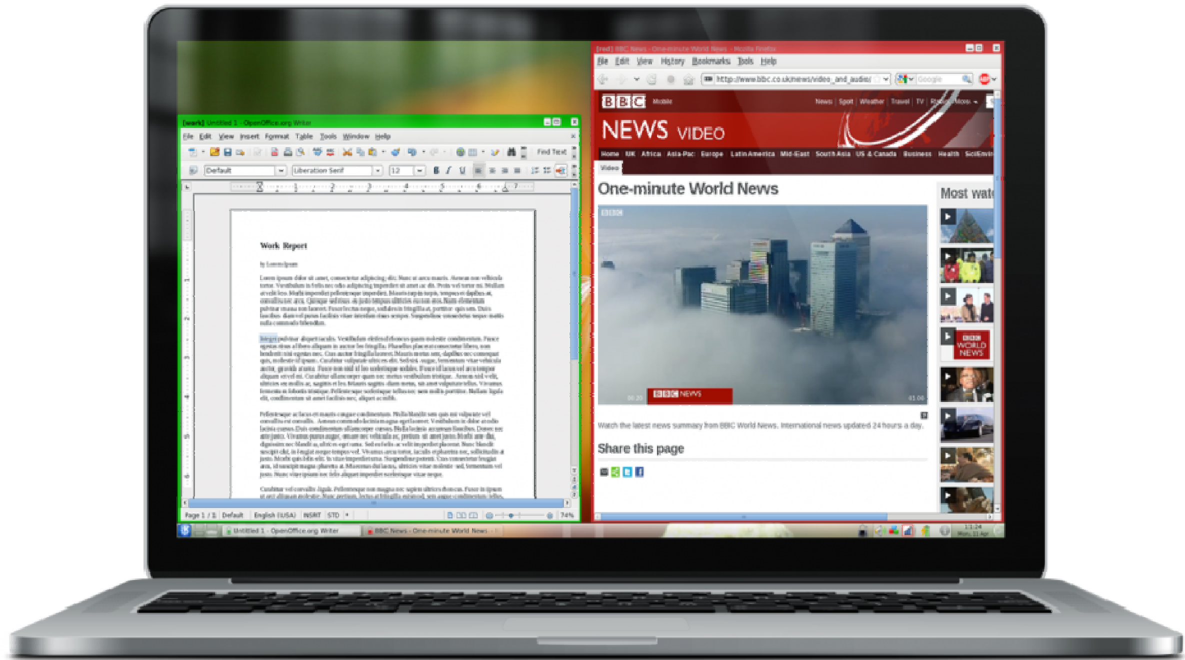
لكن عند إنشاء نافذة وهمية جديدة (**Qube**) لا يمكنك نسخ جميع ملفات **Root** (فذالك سيؤدي إلي نسخ جميع البرامج) , لكن كل نافذة وهمية **Qube** تشارك ملفات **root** مع نظيرها من قوالب الآلة الإفتراضية (**TemplateVM**) لكن كل نافذة وهمية (**Qube**) لديها صلاحية قراءة ملفات النظام **Read-Only** الموجودة داخل قالب الآلة الافتراضي المبنية عليه .. إذا النافذة الوهمية (Qube) لا تستطيع التعديل علي قالب الآلة الإفتراضي بأي شكل من الأشكال وهذا مهم جدا لأن اذا اخترقت النافذة الوهمية (**Qube**) لا يستطيع المهاجم التعديل علي قالب الآلة الافتراضي المبنيه عليه أو حتي اختراق النوافذ الوهمية الأخري (**Qubes**) المبنية علي قالب آلة افتراضي واحد فكما وضحنا سابقا أنه يمكن انشاء العديد من النوافذ الوهمية **Qubes** علي قالب آلة افتراضي واحد

.. ..

◄ عند تثبيت نظام Qubes ستلاحظ وجود بعض النوافذ الوهمية (Qubes) داخل النظام موجودة بشكل إفتراضي مثل :

- **Work** : نافذة وهمية خاصة ببيانات العمل (ان كنت تستخدم الحاسوب في العمل وتريد عزل بيانات عملك عن استخداماتك الأخري للنظام)
- **Personal** : نافذة وهمية خاصة بالإستخدام الشخصي (ان كنت تريد تصفح بريدك الشخصي او حساباتك علي مواقع التواصل الإجتماعي وعزل بياناتك الشخصية عن استخداماتك الأخري للنظام)
- **Untrusted** : نافذة وهمية " غير موثوقة " أي للاستخدام العام كتصفح المواقع الإخبارية وما شابهة

كل نافذة وهمية **Qube** لديها اسم مختلف وكذالك لون خاص لإطار النافذة الوهمية ليميزها عن بقية النوافذ الأخري فعلي سبيل المثال لون النافذة الوهمية الغير موثوقة " **Untrusted** " يكون باللون **الأحمر** كدليل علي خطورة النافذة و اللون الأخضر يرمز إلي نافذة وهمية آمنة واللون الأصفر و**البرتقالي**يرمز إلي نافذة وهمية متوسطة (ليست آمنة او غير موثوقة) واللون **الاسود** و**الازرق** يرمز إلي نافذة وهمية آمنة جدا , ويمكن تغيير الوان النوافذ واسمائها كما يريد المستخدم



كما يوجد نطاق أمني خاص يسمي " **dom0** " وذالك حيث يعمل مدير النظام ومن خلال هذا النطاق يسجل المستخدم الدخول إلي نظام التشغيل فنطاق " **dom0** " أكثر امانا من أي نطاق أخر سواء علي مستوي النوافذ الوهمية (**Qubes**) او قوالب الآلة الافتراضية (**Template VM**) فإن تم اختراق نطاق " **dom0** " فذالك يعني إختراق النظام كله ونظرا لأهمية نطاق " **dom0** " فإنه معزول بشكل إفتراضي عن الاتصال بشبكة الانترنت ويستحدم فقط لتشغيل مدير النوافذ (**Window Manager**) ومدير الحاسوب (**Desktop Manager**) ولذالك نحذر من تثبيت أي برنامج علي نطاق **dom0** او التعديل عليه

.. ..

Qubes VM Manager and Command Line Tools ➤

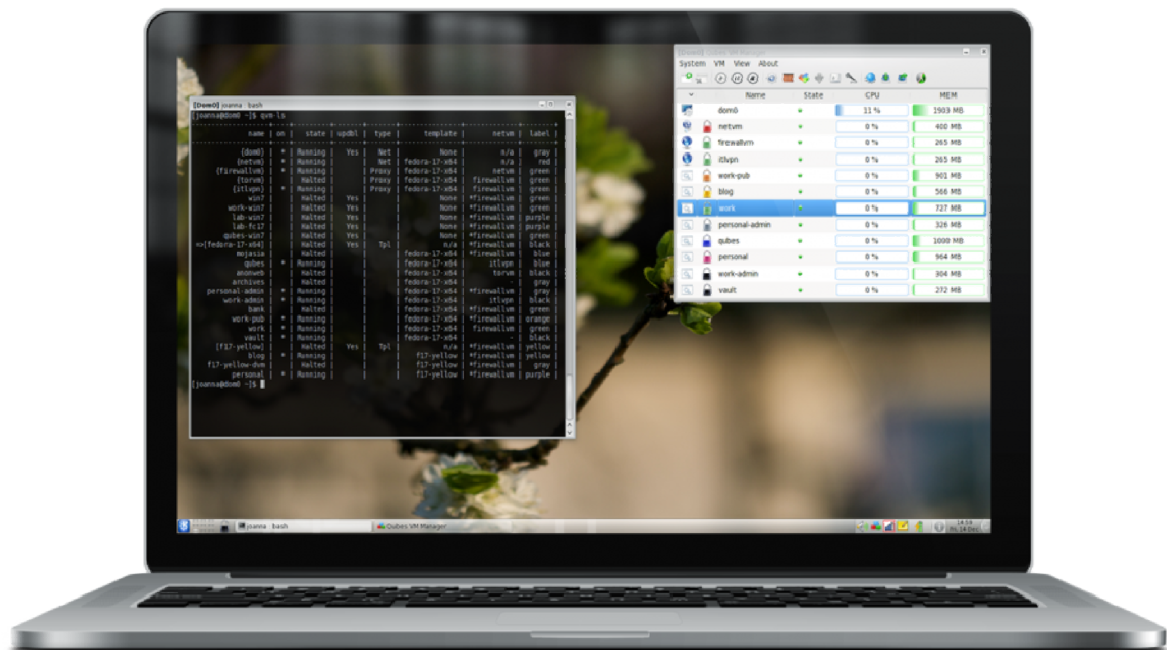
| مدير النوافذ الوهمية وأدوات سطر الأوامر |

يمكن التحكم في نظام **Qubes** بشكل كامل من خلال سطر الأوامر (**Terminal / Konsole**) في نطاق **dom0**

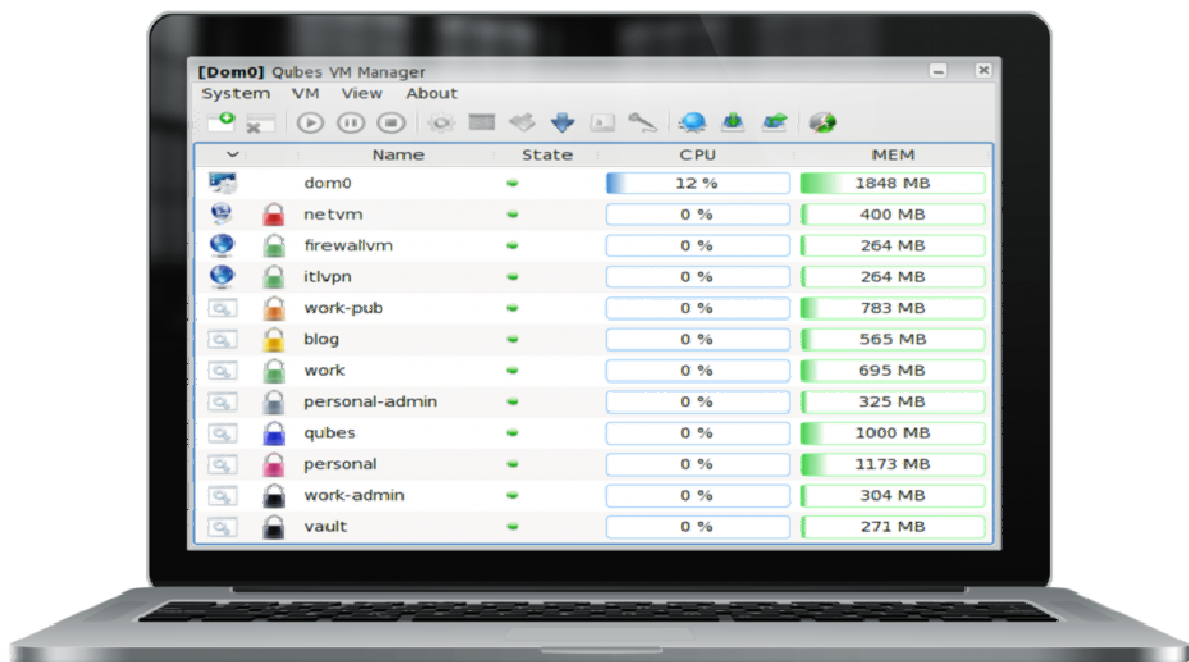
لفتح الطرفية في نطاق **dom0** إذهب الي **Start ->System Tools ->Konsole** او إضغط **Alt + F2** واكتب **Konsole**

ستجد شرح العديد من أدوات سطر الأوامر **اضغط هنا**

www.qubes-os.org/doc/dom0-tools/



ويمكن إستخدام أداة **Qubes VM Manager** لادارة النوافذ الوهمية والتحكم بها من خلال واجهة رسومية حيث تدعم جميع ادوات سطر الاوامر , أداة **Qubes VM Manager** تفتح بشكل تلقائي عند تشغيل النظام لكن يمكنك ايضا تشغيلها من خلال **Qubes Manager<- System Tools<- Start**

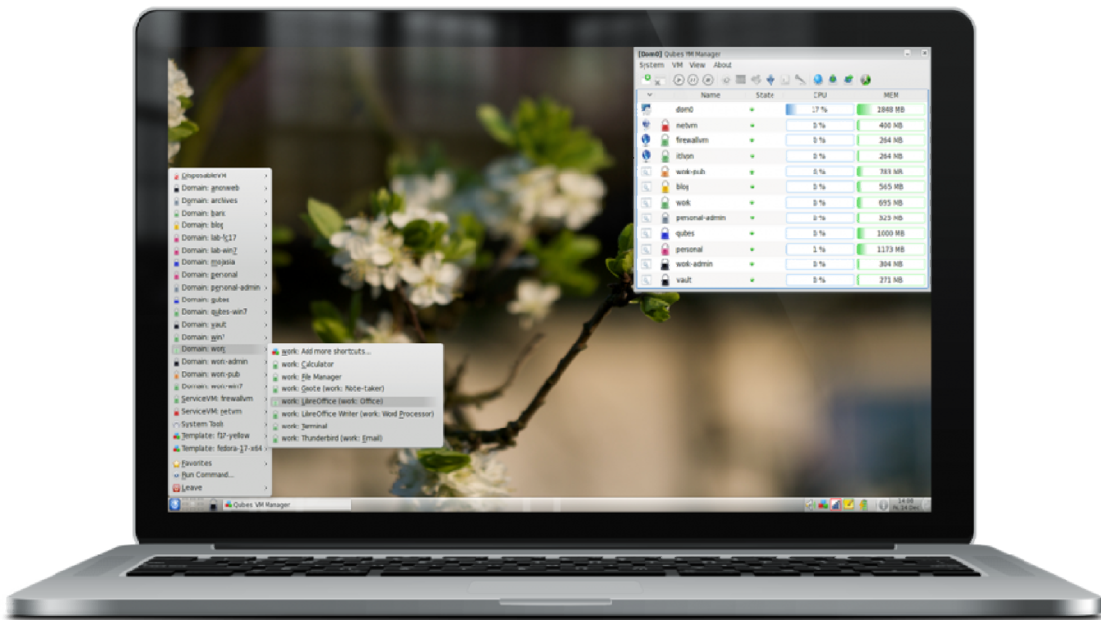


.. ..

Starting Apps in qubes ➤

تشغيل التطبيقات في| Qubes |

يمكنك تشغيل البرامج مباشرة من خلال الاختصارات الموجودة في قائمة **Desktop Manager** أو عن طريق الطرفية الموجودة بنطاق **dom0** , كما يمكنك ايضا تشغيل البرامج من قائمة ابدا حيث أن كل نافذة وهمية (**Qube**) لديها مسارات خاصة بها البرامج المثبتة كما موضح في الصورة التالية



كل نافذة وهمية (**Qube**) تحتوي بشكل تلقائي علي بعض الإختصارات , اذا اردت إضافة المزيد من الاختصارات إضغط علي **Add more Shortcuts** واختر التطبيق المراد ثم اضغط OK

كما يمكنك اضافة الاختصارات بشكل يدوي من خلال واجهة **KDE** عن طريق الضغط بزر الماوس الايمن علي قائمة ابدا ثم اختيار **Menu Editor** ثم اختر مسار النافذة الوهمية (**Qube**) التي تريد ان تظهر قائمتها ثم اضغط **New Item** ثم اكتب اسم التطبيق وامر تشغيل التطبيق كما موضح في التعليمات التالية ثم اضغط **Save** وانتظر **15**ثانية لتطبيق التحديثات

.. ..

◄ لبدء تشغيل تطبيق أو برنامج معين من الطرفية علي نطاق dom0 اكتب :

```
qvm-run -a <qube> "<app name> [arguments]"
```

- قم بإستبدال `<Qube>` بإسم النافذة الوهمية
- قم بإستبدال `<app name>` بإسم التطبيق او البرنامج

مثال لتشغيل متصفح **Firefox** داخل نافذة وهمية " **Untrusted** "

```
qvm-run -a untrusted firefox
```

.. ..

➤ Adding, Removing, and Listing qubes

| إضافة وحذف واستعراض قوائم Qubes |

يمكنك إضافة **Qube** وحذفها من خلال الضغط علي **Add** أو **Remove** في أداة **Qubes VM Manager**

كما يمكنك التعديل علي النوافذ الوهمية من خلال الطرفية علي نطاق **dom0**

- `qvm-create` || لأنشاء نافذة وهمية
- `qvm-ls` || لإستعراض نافذة وهمية
- `qvm-remove` || لحذف نافذة وهمية

» كان ذالك مدخل لنظام Qubes OS ذكرنا فيه أساسيات نظام التشغيل

وسوف نتابع نشر سلسلة مقالات في الايام القادمة بإذن الله حول نظام Qubes نظرا لأهميته «

——.——.——.——.——.——.——.——.——

واخر دعوانا أن الحمدلله رب العالمين



Horizons

مؤسسة آفاق الإلكترونية

للتواصل:

 @TECH_SUPPORT

 @SR444TAW